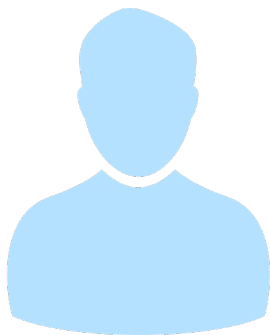


What you most likely did not know about sudo...

Peter Czanik / One Identity (Balabit)



About me



- Peter Czanik from Hungary
- Open Source Evangelist at One Identity -- home of syslog-ng and patron of sudo
- syslog-ng packaging, support, advocacy

syslog-ng originally developed by Balabit, now part of One Identity

Overview

- What is sudo
- From aliases to plugins
- Alerting with syslog-ng

What is sudo?

- Depending on experience and size of environment:
 - A tool to complicate life
 - A prefix for administrative commands
 - A way to see who did what

What is sudo?

- Sudo allows a system administrator to delegate authority by giving certain users the ability to run some commands as root or another user while providing an audit trail of the commands and their arguments. (<https://www.sudo.ws/>)
- A lot more, than just a prefix

Basic /etc/sudoers

```
%wheel ALL=(ALL) ALL
```

- Who
- Where
- As which user
- Which command

Aliases

- Aliases:
 - Simplify configuration
 - Less error-prone

Host_Alias WEBSERVERS = www1, www2, www3

User_Alias ADMINS = millert, dowdy, mikef

Cmnd_Alias REBOOT = /sbin/halt, /sbin/reboot, /sbin/poweroff

ADMINS WEBSERVERS = REBOOT

Defaults

- Changes the default behavior:

Defaults secure_path="/usr/sbin:/usr/bin:/sbin:/bin"

Defaults env_keep = "LANG LC_ADDRESS LC_CTYPE"

Defaults !insults

- Can be user/host/etc specific

Defaults:%wheel insults

Insults

- Fun, but not always PC :)

```
czanik@linux-mewy:~> sudo ls
```

```
[sudo] password for root:
```

```
Hold it up to the light --- not a brain in sight!
```

```
[sudo] password for root:
```

```
My pet ferret can type better than you!
```

```
[sudo] password for root:
```

```
sudo: 3 incorrect password attempts
```

```
czanik@linux-mewy:~>
```

Digest verification

```
peter ALL =  
sha244:11925141bb22866afdf257ce7790bd6275feda80b3b241c108b  
79c88 /usr/bin/passwd
```

- Modified binaries do not run
- Difficult to maintain
- Additional layer of protection

Session recording

- Recording the terminal
- Play it back
- Difficult to modify (not cleartext)
- Easy to delete (saved locally) with unlimited access

Session recording

- Demo

Plugin-based architecture

- Starting with version 1.8
- Replace or extend functionality
- Both open source and commercial

Plugin-based architecture

- Demo of sudo_pair
- Making sure that no user can enter commands on their own
- Developed in Rust
- https://github.com/square/sudo_pair/

Configuration

- Read from top to bottom
- Start with generic
- Add exceptions at the end

Central management

- Puppet, Ansible, etc.
 - Not real-time
 - Users can modify locally
 - Error-prone
- LDAP
 - Propagates real-time
 - Can't be modified locally
 - Many limitations

Sample configuration

```
Defaults !visiblepw
Defaults always_set_home
Defaults match_group_by_gid
Defaults always_query_group_plugin
Defaults env_reset
Defaults env_keep = "COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS"
Defaults env_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE"
Defaults secure_path = /sbin:/bin:/usr/sbin:/usr/bin
root    ALL=(ALL)    ALL
%wheel ALL=(ALL)    ALL
Defaults !insults
Defaults:%wheel insults
Defaults log_output
Host_Alias WEBSERVERS = www1, www2, www3
User_Alias ADMINS = millert, dowdy, mikef
Cmnd_Alias REBOOT = /sbin/halt, /sbin/reboot, /sbin/poweroff
ADMINS WEBSERVERS = REBOOT
```

Logging and alerting

- E-mail alerts
- All events to syslog
 - Make sure logs are centralized
 - Using syslog-ng sudo logs are automatically parsed and you can also do alerting to Slack, Splunk, Elasticsearch, etc.
- Debug logs
 - Debug rules
 - Report problems

syslog-ng

- Logging

Recording events, such as:

```
Jan 14 11:38:48 linux-0jbu sshd[7716]: Accepted publickey for root  
from 127.0.0.1 port 48806 ssh2
```

- syslog-ng

Enhanced logging daemon with a focus on portability and high-performance central log collection. Originally developed in C.

Configuring syslog-ng

- “Don't Panic”
- Simple and logical, even if it looks difficult at first
- Pipeline model:
 - Many different building blocks (sources, destinations, filters, parsers, etc.)
 - Connected into a pipeline using “log” statements

syslog-ng.conf: getting started

```
@version:3.19
```

```
@include "scl.conf"
```

```
# this is a comment :)
```

```
options {flush_lines (0); keep_hostname (yes);};
```

```
source s_sys { system(); internal();};
```

```
destination d_mesg { file("/var/log/messages"); };
```

```
filter f_default { level(info..emerg) and not (facility(mail)); };
```

```
log { source(s_sys); filter(f_default); destination(d_mesg); };
```

syslog-ng.conf: sudo building blocks

```
filter f_sudo {program(sudo)};
```

```
destination d_test {  
  file("/var/log/sudo.json"  
  template("${format-json --scope nv_pairs --scope dot_nv_pairs --scope rfc5424}\n\n"));  
};
```

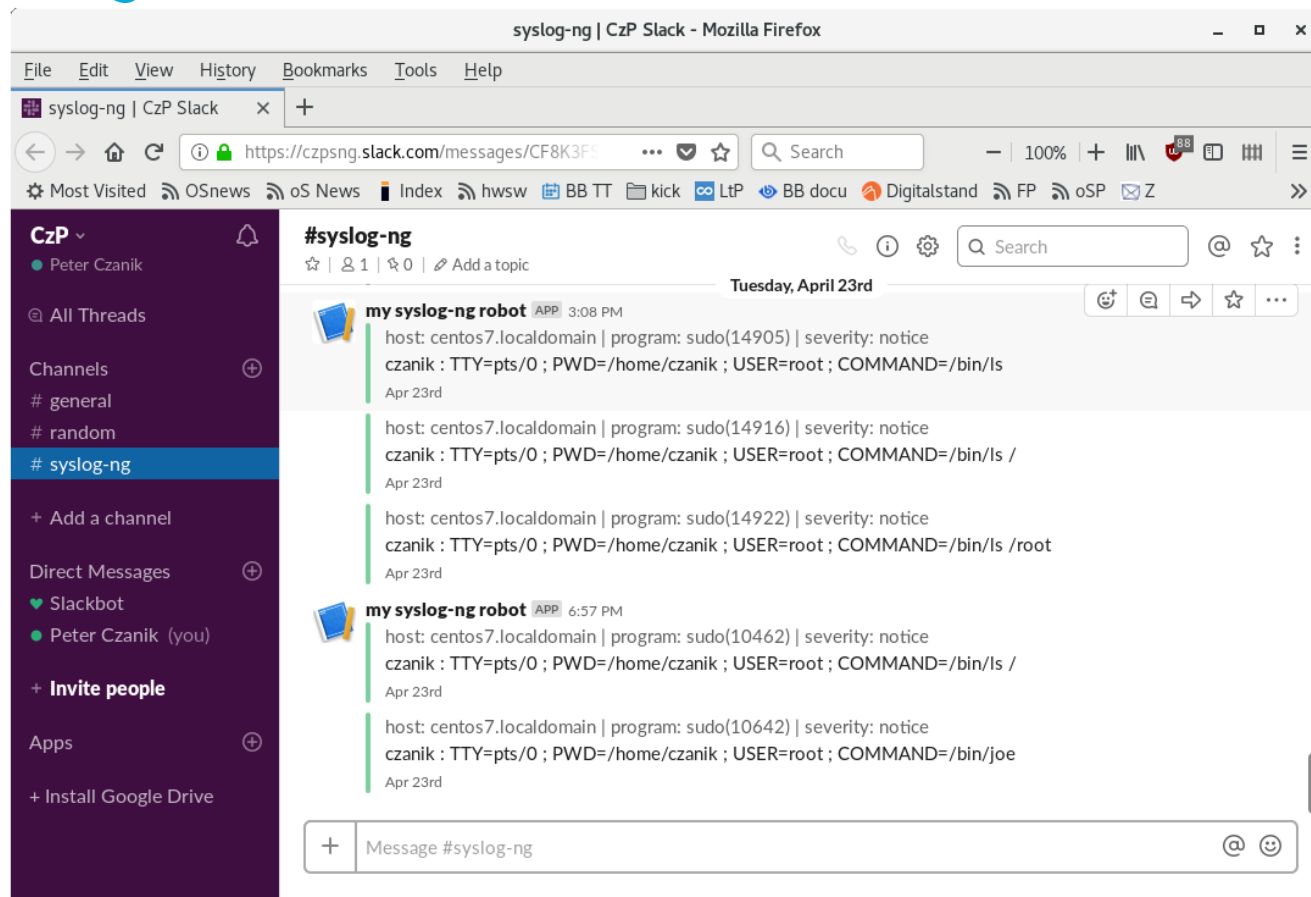
```
destination d_slack {  
  slack(hook-url("https://hooks.slack.com/services/TF8LZ3CSF/BF8CJKVT3/  
C2qdnMXCwDD3ATOFVMyxMyHB")  
  );  
};
```

syslog-ng.conf: sudo log statement

name-value pairs come from the sudo parser

```
log {  
    source(s_sys);  
    filter(f_sudo);  
    if (match("czanik" value(".sudo.SUBJECT"))) {  
        destination { file("/var/log/sudo_filtered"); };  
        destination(d_slack);  
    };  
    destination(d_test);  
};
```

sudo logs in Slack



The screenshot shows a Slack interface in a Mozilla Firefox browser window. The browser address bar shows the URL `https://czpsng.slack.com/messages/CF8K3FS`. The Slack channel is `#syslog-ng`. The channel sidebar on the left shows the user `Peter Czanik` and a list of channels including `#syslog-ng`. The main chat area displays a series of log messages from a bot named `my syslog-ng robot`. The messages are timestamped `Tuesday, April 23rd` and contain the following log entries:

```
host: centos7.localdomain | program: sudo(14905) | severity: notice
czanik : TTY=pts/0 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/ls
Apr 23rd

host: centos7.localdomain | program: sudo(14916) | severity: notice
czanik : TTY=pts/0 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/ls /
Apr 23rd

host: centos7.localdomain | program: sudo(14922) | severity: notice
czanik : TTY=pts/0 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/ls /root
Apr 23rd

host: centos7.localdomain | program: sudo(10462) | severity: notice
czanik : TTY=pts/0 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/ls /
Apr 23rd

host: centos7.localdomain | program: sudo(10642) | severity: notice
czanik : TTY=pts/0 ; PWD=/home/czanik ; USER=root ; COMMAND=/bin/joe
Apr 23rd
```

The input field at the bottom of the chat area contains the text `Message #syslog-ng`.

Not just a prefix, but...

- Fine tuned permissions
- Aliases
- Defaults
- Digest verification
- Session recording
- LDAP
- Plugins
- Logging and alerting



Questions?

sudo website: <https://www.sudo.ws/>

My e-mail: peter.czanik@oneidentity.com

Twitter: <https://twitter.com/PCzanik>

